FILED

OCT 25 2024

Heidi D. Campbell, Clerk
U.S. DISTRICT COURT

AO-106 (Rev: 06/09)-Application for Search Warrant

UNITED STATES DISTRICT COURT

for the

Northern District of Oklahoma

In the Matter of the Search of *Information Associated with Facebook Accounts 61550038546748, 100027927924028, And 1843835659471281 that are Stored at Premises Controlled By Meta Platforms, Inc*	)	Case No. 24-mj-674-SH **FILED UNDER SEAL**

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment "A." This court has authority to issue this warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A).
located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized):*

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 875(c)	**Interstate Communications**
18 U.S.C. § 2261A(2	**Cyberstalking**

The application is based on these facts:

See Affidavit of Casey S. Cox, attached hereto.

☑ Continued on the attached sheet.

☐ Delayed notice of ___ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Casey S. Cox
Applicant's signature

Casey S. Cox, FBI
Printed name and title

Subscribed and sworn to by phone.

Date: 10/25/24

Susan E. Huntsman
Judge's signature

City and state: Tulsa, Oklahoma

Susan E. Huntsman, U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OKLAHOMA

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH FACEBOOK ACCOUNTS 61550038546748, 100027927924028, AND 1843835659471281 THAT ARE STORED AT PREMISES CONTROLLED BY META PLATFORMS, INC.	Case No. **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Casey S. Cox, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the United States Department of Justice, Federal Bureau of Investigation (FBI), and have been so employed since October 2006. I am currently assigned to the Oklahoma City Division of the FBI, Civil Rights and Public Corruption Squad. I have primary investigative responsibility for criminal civil rights violations, which include allegations of bias or gender motivated threats, intimidation, and harassment in violation of 18 U.S.C. § 875(c) [Interstate Communications] and 18 U.S.C. § 2261A(2) [Cyberstalking].

2. I make this affidavit in support of an application for a search warrant for information associated with certain accounts, that are stored at premises owned, maintained, controlled, or operated Meta Platforms, Inc. ("Meta"), a company headquartered in Menlo Park, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Meta to disclose to the government

records and other information in its possession, pertaining to the subscriber or customer associated with the accounts, which are further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not set forth all of my knowledge about this matter. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary for the limited purpose of establishing probable cause to conduct a search of and for the items described in Attachments A and B for evidence, contraband, and/or instrumentalities of the criminal conduct described herein. Additionally, unless otherwise indicated, wherever in this affidavit I assert that an individual made a statement, that statement is described in substance herein and is not intended to be a verbatim recitation of such statement. Furthermore, unless otherwise indicated, all statements contained in this affidavit are summaries in substance and in part. The following is true to the best of my knowledge and belief.

4. Based on my training and experience and the facts set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 875(c) [Interstate Communications] and 18 U.S.C. § 2261A(2) [Cyberstalking] have been

committed, are being committed, AND/OR will be committed by John Gregory Garza [the **"Target"**], aka "Mikey Chuddington", aka "Mike Chuddington", aka "Mike Chudington", aka "Chud Rosenberg", and aka "Cole McHale". There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

BACKGROUND OF INVESTIGATION DEFINITIONS AND TECHNICAL TERMS

6. Based on my training and experience, and information acquired from other law enforcement officials with technical expertise, I know the terms described below have the following meanings or characteristics:

7. A provider of "Electronic Communication Service" ("ESP"), as defined in 18 U.S.C. § 2510(15), is "any service that provides to users thereof the ability to send or receive wire or electronic communications." For example, "telephone companies and electronic mail companies" generally act as providers of electronic

communication services. *See* S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3568.

8. Instant messaging (IM) is a collection of technologies that create the possibility of real-time text-based communication between two or more participants via the Internet. Instant messaging allows for the immediate transmission of communications, including immediate receipt of acknowledgment or reply.

9. Internet Protocol Address: An Internet Protocol address (IP address) is a unique numeric address used by computers on the Internet. An IP Address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. An IP address acts much like a home or business street address -- it enables computers connected to the Internet to properly route traffic to each other. The assignment of IP addresses to computers connected to the Internet is controlled by Internet Service Providers (ISPs).

10. An IP address is a number that uniquely identifies internet-connected computers. When one computer interacts with a second computer over the internet, the first computer communicates its IP address to the second computer, so that each computer can communicate with the other. The system of IP addresses is managed by the Internet Corporation For Assigned Names and Numbers ("ICANN"), together with five Regional Internet Registries (essentially, one for each populated continent except Australia, which is combined with most of Asia), including the

American Registry for Internet Numbers ("ARIN"), which has responsibility for North America. ARIN registers IP addresses for internet-connected computers in North America and maintains records about the registered owners for those IP addresses. ARIN registered owners are typically large users or organizations, such as remote computing or internet service providers (e.g., Comcast), who can internally assign IP addresses to computers that belong to individual subscribers.

11. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

PROVIDER BACKGROUND[1]

12. Meta owns and operates Facebook, a free-access social networking website that can be accessed at http://www.facebook.com. Facebook users can use their accounts to share communications, news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

13. Meta asks Facebook users to provide basic contact and personal identifying information either during the registration process or thereafter. This information may include the user's full name, birth date, gender, e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen

[1] The information in this section is based on my training and experience, and on information published by Meta on its Facebook website, including, but not limited to, the following webpages: "Privacy Policy," available at https://www.facebook.com/privacy/policy; "Terms of Service," available at https://www.facebook.com/legal/terms; "Help Center," available at https://www.facebook.com/help; and "Information for Law Enforcement Authorities," available at https://www.facebook.com/safety/groups/law/guidelines/.

names, websites, and other personal identifiers. Each Facebook user is assigned a user identification number and can choose a username.

14. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

15. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create "lists" of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

16. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status"

updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. In addition, Facebook users can "check in" to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user's profile page also includes a "Wall," which is a space where the user and his or her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

17. Facebook users can upload photos and videos to be posted on their Wall, included in chats, or for other purposes. Users can "tag" other users in a photo or video, and can be tagged by others. When a user is tagged in a photo or video, he or she generally receives a notification of the tag and a link to see the photo or video.

18. Facebook users can use Facebook Messenger to communicate with other users via text, voice, video. Meta retains instant messages and certain other shared Messenger content unless deleted by the user, and also retains transactional records related to voice and video chats, including the date of each call. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile.

19. If a Facebook user does not want to interact with another user on Facebook, the first user can "block" the second user from seeing his or her account.

20. Facebook has a "like" feature that allows users to give positive feedback or connect to particular pages. Facebook users can "like" Facebook posts or updates, as well as webpages or content on third-party (i.e., non-Facebook) websites. Facebook users can also become "fans" of particular Facebook pages.

21. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

22. Each Facebook account has an activity log, which is a list of the user's posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as "liking" a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user's Facebook page.

23. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

24. In addition to the applications described above, Meta provides users with access to thousands of other applications ("apps") on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user's access or use of that application may appear on the user's profile page.

25. Meta also retains records of which IP addresses were used by an account to log into or out of Facebook, as well as IP addresses used to take certain

actions on the platform. For example, when a user uploads a photo, the user's IP address is retained by Meta along with a timestamp.

26. Meta retains location information associated with Facebook users under some circumstances, such as if a user enables "Location History," "checks-in" to an event or location, or tags a post with a location.

27. Social networking providers like Meta typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Meta about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Meta typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

28. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user's IP log, stored electronic communications, and other data retained by Meta, can indicate who has used or controlled the Facebook account. This "user attribution" evidence is

analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Meta logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, location information retained by Meta may tend to either inculpate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner's state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

29. Therefore, the servers of Meta are likely to contain all the material described above, including stored electronic communications and information

concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

FACTS ESTABLISHING PROBABLE CAUSE

30. The United States is investigating the transmission of bias or gender motivated threats to injure, including threats to rape adult female victims and unborn children, as well as patterns of conduct (also referred to as course of conduct) committed with the intent to harass and intimidate female victims, and male partners of those female victims, via interstate or foreign commerce. The investigation concerns possible violations of, inter alia, 18 U.S.C. § 875(c) and 18 U.S.C. § 2261A(2).

31. Victim 1, an adult white female, is married to Victim 2, an adult Hispanic male. Victim 1 and Victim 2 are expecting a baby. Victim 1 and Victim 2 both reside in Tulsa, Oklahoma, which is within the Northern District of Oklahoma. Victim 1 and Victim 2 received threatening communications while residing in Tulsa, Oklahoma.

32. On June 8th, 2024, Victim 1 received direct threatening communications on her Facebook account over Facebook Messenger from Facebook user: "Mikey Chuddington". Specifically, Facebook user "Mikey Chuddington" threatened to rape not only Victim 1, but also her unborn child.

33. On June 8th, 2024, Victim 1's husband (Victim 2) also received racist messages via Facebook Messenger from Facebook user "Mikey Chuddington" over Facebook Messenger. Facebook user "Mikey Chuddington" called Victim 2 a

"*Nigger*" and called Victim 1 a "*mudshark*". Victim 2 was told via Facebook Messenger to "*Stick to your own race ng er*". "*Filthy animal*". Victim 1 provided a screen shot to the investigating agent showing the comment to Victim 2 regarding sticking to his own race.

34. Also, on that same day, June 8th, 2024, Facebook user "Mikey Chuddington" re-posted a post from Victim 1 to the user's own Facebook account, along with the comment "*Stanford Norrel Ethan Cuckier if I hold her down do you think you can make her bleed?*" Within the comment, "*Stanford Norrel*" and "*Ethan Cuckier*" were tagged Facebook users by those names. Victim 1 provided a screen shot of this comment to the investigating agent.

35. Also, on that same day, June 8th, 2024, Facebook user "Mikey Chuddington" shared Victim 1's profile picture and added the captions "*rape time*" and "*can't wait to meet you*". Facebook user "Mikey Chuddington" then tagged Victim 2 in the comments saying, "*keep that baby safe she is going to get raped*".

36. Throughout the remainder of June 8th, 2024, Facebook user "Mikey Chuddington" continued to send threatening posts to Victim 1 stating, among other things, that he was going to make Victim 1's "*asshole bleed*". The specific post by Facebook user "Mikey Chuddington" stated "*Make her a sshole bleed*" was posted above to a picture posted by Victim 1 on March 18th, 2024, showing Victim 1 in a neck brace and a link to a GoFundMe page titled "Support [Victim 1] and unborn baby after car accident, organized by [Victim 1]". Victim 1 posted on March 27th,

2024 "The best day of my life". On June 8th, 2024, Facebook user "Mikey Chuddington commented to this post saying, "*She's going to get r aped*".

37. Per Victim 1, Facebook user "Mikey Chuddington" also shared on his Facebook account pictures of other interracial couples and called them racial slurs. Victim 1 felt Facebook user "Mikey Chuddington's" posts/comments were threatening and racially motivated.

38. Also on June 8th, 2024, following the transmission of these threats, intimidation, and harassment from Facebook user "Mikey Chuddington" to Victim 1 and Victim 2, Victim 1 was contacted via Facebook Messenger by Victim 3, an adult white female, who is a stranger to the Facebook user "Mikey Chuddington". Victim 3 resides in Tulsa, Oklahoma, which is within the Northern District of Oklahoma. Victim 3 received threatening communications while residing in Tulsa, Oklahoma. Victim 3 sent Victim 1 screen shots of Facebook user "Mikey Chuddington's" Facebook page comments where he mentioned he was going to rape Victim 1. Victim 1 provided the investigating agent copies of the screen shots that Victim 3 sent her.

39. The screenshots that Victim 1 provided to the investigating agent also contain threats, intimidation, and harassment directed at Victim 3. On June 8th, 2024, Facebook user "Mike Chuddington" posted on his Facebook page "*R ape like a dog*" above a video posted by Facebook user "Mrs Oklahoma Pageant". Victim 3 was in the video posted by "Mrs. Oklahoma Pageant". Specifically, in the screenshots, Facebook user "Mikey Chuddington" told Victim 3 through comments posted on

Victim 3's Facebook page that she "[Victim 3] *won't survive*" and "*Somebody special knows where you live. Prepare.*" Facebook user "Mikey Chuddington" also commented to Victim 3 that "[*Victim 1*] *is gonna get r aped like an animal can't wait*".

40. On October 18th, 2024, the investigating agent spoke with Victim 3 who was able to provide a recording of Facebook Messenger communications between Victim 3 and Victim 1 which occurred on June 8th, 2024. Victim 3 told Victim 1 that she had received some concerning posts with her name attached and wanted to give her a heads up. Victim 3 included screen shots of the posts by Facebook user "Mike Chuddington" [These were the same screen shots provided to the investigating agent by Victim 1]. Victim 3 advised she did not know who the Facebook user was and had blocked him. Victim 1 replied to Victim 3 "*I know he's been threatening my husband and I all day and I'm so scared*". Victim 3 asked if they were also in Oklahoma and Victim 1 replied, "*Yes, we are but I can't tell if he is or not*". Victim 3 also asked Victim 1 if she knew him and Victim 1 replied, "*Never talked to him in my life. He messaged my husband and started saying racial slurs. I can show you*". Victim 1 then shared a screen shot of the Facebook Messenger comment sent by "Mikey Chuddington" to Victim 2 [This screen shot was also provided to the investigating agent by Victim 1]. Victim 1 went on to tell Victim 3, "*I'm also pregnant and he threatened to rape my baby*". Victim 3 advised he was threatening her and was tagging Victim 1's name in Victim 3's Facebook page and sharing Victim 3's post as his and making rape comments. Victim 1 and Victim 3 continued to talk about how they hope he [Mikey

Chuddington] is not in Oklahoma and Victim 3 tells Victim to "*Please be careful and watch your back*".

41. Victim 1 was able to identify the Facebook account for Facebook User "**Mikey Chuddington**" as https://facebook.com/profile.php?ID=61550038546748 (hereinafter, "**Target Account 1**"). A preservation request was sent to Meta Platforms, Inc. on June 25th, 2024, for **Target Account 1**.

42. The investigation has also identified other Facebook accounts, an Instagram account, a Threads account, and a X account[2], which are associated with Facebook user "Mikey Chuddington". Publicly available posts on these accounts show posts calling for legalizing rape and antisemitic views. The second Facebook account identified is **https://facebook.com/cole.mchale.5, username: "Chud Rosenberg**", and user **ID: 100027927924028** (hereinafter, "**Target Account 2**"). The Instagram account is identified as https://instagram.com/mikechudington, username: "Mikey Chuddington", user ID: @mikechudington. On March 10th, 2024, three months before Victim 1 received threats of rape to herself and her unborn child from **Target Account 1** Facebook user "Mikey Chuddington", Facebook user "Chud Rosenberg" posted a video on **Target Account 2** and Instagram user "Mikey Chuddington" posted the same video on his Instagram account. The video posted to both accounts begins with a music concert with "Dance Gavin Dance" behind the band, but approximately eight seconds into the video another video shows up

[2] Threads is a social media platform also owned by Meta Platforms, Inc. and X is a social media platform previously known as Twitter.

underneath the video of the band. The video that appears underneath is a video of Elliot Rodgers giving his manifesto prior to conducting a mass shooting in California in 2014. Of relevance, the investigating agent is aware that Rodgers specifically targeted women in his mass shooting event and has since become an icon and inspiration within a specific online community.

43. On July 24th 2024, **Target Account 2** shared a post from **Target Account 1,** further supporting that the user of these two accounts could be the same person. On June 22nd, 2024, Instagram User "Mikey Chuddington" posted on his Instagram account, a meme[3] posted with the message "*Tfw* [that feeling when] *rape is finally Finally LEGAL*".

44. On August 10th, 2024, **Target Account 2** Facebook user "Chud Rosenberg" commented "*Let me find someone asleep like this. Their asshole is gonna be bloody*" to a post by a female Facebook user who posted a meme of an unknown female lying face down on a bed wearing a short skirt with the caption under the picture saying, "me as soon as I get home from anywhere".

45. On August 19th, 2024, the investigating agent served Meta Platforms, Inc. with a 2703(d) order for Facebook accounts: **61550038546748 (username: Mikey Chuddington) (Target Account 1)** and **100027927924028 (username: Chud Rosenberg) (Target Account 2)**. A 2703(d) order was also served to Meta Platforms, Inc. for the Instagram account @mikechudington (username: "Mikey

[3] A "meme" is a cultural item that is shared and spread via the Internet and can be an image, a video, a GIF, or other format.

Chuddington"). On August 26th, 2024, Facebook provided records pursuant to the 2703(d) order. The records did not identify a potential true name but provided Internet Protocols (IP) addresses associated with posts from the Facebook accounts that appeared to originate from Chicago, Illinois. On August 30th, 2024, Instagram provided records pursuant to the 2703(d) order. Identified in the records provided by Instagram was the email "JohnGregoryGarza@gmail.com" used to register [create] the Instagram account in August 2023. Also identified were IP addresses that, like the Facebook accounts, appeared to originate from Chicago, Illinois.

46. A Threads account was identified linked with the Instagram account used by "mikechudington". On July 5th, 2024, Threads user "Mikechudington" replied to a photograph posted by user "abelinasabrina", stating "*Stick to your o*wn r*ace*". The photograph was of a female standing next to a male with their backs towards the camera while looking over a wall. On August 12th, 2024, Threads user "jesusxcraves" replied to user "Mikechudington" stating "*okay incel*[4] *confirmed possible p0rn addict cannot be verified yet but have fun being a predator!*" User "Mikechudington" replied "'*I'm a porn addict' despite having a girlfriend fearing God etc. all this because my girlfriend is 17 and 6 months. Your boyfriend is attracted to you because you resemble an indigenous child his ancestors would r ape/m urder in the jungle. No man is attracted to something like you unless they have serious problems/what I already explained. Keep coping. Ape. Disgrazia* ["disgrazia" is an Italian word that translates to "disgrace"]". Threads

[4] "Incel" is short for "involuntary celibate" and refers to a loosely organized community of men who believe that they have been unfairly denied sexual or romantic attention from women. These beliefs can translate into an animus toward women and a desire for revenge through violence against women.

user "mikechudington" commented again to user "jesusxcraves" stating "*Let me tell you something babe. As a white man, I can say your boyfriend likes you cause you're brown and the size of a grade schooler. He fetishizes you. Probably because he had a Latina porn addiction long before he met you. Many such cases. My girlfriend although is 17 doesn't look like a child. I don't like her cause of her age. Although your bf likes you cause you remind him of an indigenous child in the wilderness lmao* [laugh my ass off]". That same day, August 12th, 2024, Threads user "pinguicha" posted "*I don't understand how grown-ass men look at teenagers and think, "That's a fully grown woman*"". Threads user "mikechudington" replied "*I'm 24 and I'm with a 17 yr old (legal here) it's amazing*".

47. On August 22nd, 2024, **Target Account 1** Facebook user "Mikey Chuddington" posted "*When I'm taken into custody for a mass m urder they're going to report "the perpetrator posted that morning on Facebook "good frankleee morning frens"…*" On August 25th, 2024, **Target Account 1** Facebook user "Mikey Chuddington" posted "*Butt fuck u nderage women*".

48. The investigating agent was made aware of a third Facebook account associated with username "Mikey Chuddington". This Facebook account also has publicly available posts. On August 26th, 2024, **Facebook account 1843835659471281 username "Mikey Chuddington"** (hereinafter "**Target Account 3**") posted "*Everyday I become more and more like Chris Benoit and that's not a joke*". The investigating agent is aware that Chris Benoit was a professional wrestler who murdered his wife and son and then committed suicide in 2007. That same day,

August 26th, 2024, **Target Account 3** Facebook user "Mikey Chuddington" also posted "*I'm gonna h urt myself and others*". The investigating agent observed publicly available comments to this post on **Target Account 3** for Facebook user "Mikey Chuddington" to harm himself and others. One such comment included Facebook user "Ethan Cook" asking "*Are you meeting dillian*". In response to this question on **Target Account 3**, Facebook user "Stanford Norrel" replied "Yuuuup" and user "Mikey Chuddington" replied "*Up*". The investigating agent believes the response of "*Up*" was either a typo or shorthand for "Yup" by Facebook user "Mikey Chuddington". [Of note, as stated above in paragraph 34, **Target Account 1** Facebook user "Mikey Chuddington" communicated with Facebook user "Standford Norrel" on June 8th, 2024, when he posted a Facebook comment that asked Facebook user "Stanford Norrel" whether if he [Chuddington], held down Victim 1, Norrel could make her bleed. The fact that **Target Account 1** Facebook user "Mikey Chuddington" and **Target Account 3** Facebook user "Mikey Chuddington" communicated with the same Facebook user, "Stanford Norrel", about ideations of rape and, as described below, believed ideations of biased-motivated mass shootings, supports that Facebook user "Mikey Chuddington" is the same person for each target account.]. Further, the investigating agent believes that comment on **Target Account 3** about Facebook user "Mikey Chuddington" meeting "dillian" this is a reference to Dylann Roof (Roof). Roof was a mass murder who killed nine people inside a Charleston, South Carolina church in a bias-motivated

mass shooting, admitting he was hoping to incite a race war. Roof was convicted of federal hate crime violations resulting in death with the use of a firearm and is currently in a federal prison awaiting execution. Of note, Roof is also mentioned in other posts made by **Target Account 3** Facebook user "Mikey Chuddington". A preservation request was sent to Meta Platforms, Inc. on August 28th, 2024, for Facebook account **1843835659471281, Target Account 3**.

49. On September 4th, 2024, a federal Grand Jury subpoena was served on T-Mobile requesting subscriber information related to Internet Protocol (IP) addresses associated with postings from the identified Facebook accounts **Target Accounts 1, 2, and 3** as well as the Instagram account used by Facebook user "Mikey Chuddington". These IP addresses were identified from the 2703(d) returns provided by Meta Platforms, Inc. On September 19th, 2024, T-Mobile provided records responsive to the federal Grand Jury subpoena. The records indicate the user of the Facebook accounts **Target Accounts 1, 2, and 3** and the Instagram account is likely John Gregory Garza, who resides in Chicago, Illinois. A date of birth was also identified for John Gregory Garza identifying him as being 24 years old. This is the same age that Threads user "mikechudington" identified in his post described above on August 12th, 2024. Telephone number 312-690-1001 was identified from the 2703(d) returns as being associated with both Facebook accounts **61550038546748 (Target Account 1)** and **100027927924028 (Target Account 3)**. This telephone number was used by the Facebook accounts holder to verify [responded to a text

message sent from Facebook] the accounts when they were registered. The same telephone number (312-690-1001) was also identified with the T-Mobile subpoena return associated with subscriber John Gregory Garza. Therefore, Facebook account content provided pursuant to this search warrant will likely help to further identify the true identity of the user of the Facebook accounts as well as identify other threatening communications which will assist with identifying other victims that have been threatened by the user of the Facebook accounts using the vanity names: "Mikey Chuddington" and "Chud Rosenberg" and believed to be John Gregory Garza.

50. In addition, there is probable cause to believe that **Target Accounts 1, 2, and 3**, contain evidence of the offenses under investigation in data and content preceding the commission of the offenses under investigation. Based on my training and experience, I know that individuals who hold bias-motivated views, including racially biased and gender biased views, and who act on those views, making, such as here, bias or gender motivated threats, intimidation, and harassment develop biased belief systems, and the motivation to act on those beliefs, over time. Here in particular, **Target Account 2** Facebook user "Chud Rosenberg" and Instagram user "Mikey Chuddington" (both of whom have been connected through evidence to **Target Account 1** user "Mikey Chuddington" and **Target Account 3** user "Mikey Chuddington", suggesting they are all the same person) publicly posted a video of a mass murderer idealizing violence against women months before **Target Account 1**

Facebook user "Mikey Chuddington" sent direct threats over Facebook Messenger to Victim 1 to rape her and her unborn baby. Thus, the evidence supports that Facebook user "Mikey Chuddington" and "Chud Rosenberg", believed to be John Gregory Garza [the **Target**], held idealizations of violence against women that preexisted the threats, harassment, and intimidation under investigation, and in my training and experience, it is likely that evidence of the target's beliefs about gender and race will be found in **Target Accounts 1, 2, and 3**, in the months preceding his decision to publicly post these beliefs and, evidently based on this belief, begin threatening multiple victims with physical harm.

51. Finally, in my training and experience, if a target, such as John Gregory Garza [the **Target**], is comfortable publicly posting about his bias and racially motivated views as well as desire to commit violent rapes, it is exceedingly likely that his Facebook accounts will contain other evidence of his intent with respect to violence against women, interracial couples, racism, and his motive to commit the offenses under investigation. For example, in my training and experience, I know that individuals who commit bias-motivated crimes and make bias-motivated statements publicly on social media are likely to also reveal their belief systems in non-public posts or comments; in private messages; in comments, reactions to, or sharing of others' posts, photos, videos, events, or the like; in comments, reactions to, or sharing of articles or information; in records of groups or events joined or followed; and the like. There is thus probable cause to believe that evidence of intent could be found in any of these categories.

REQUEST FOR SEALING

52. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the Internet and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

REQUEST FOR NON-DISCLOSURE

53. Request for Order Barring Notification of Other Persons (Non-Disclosure Order): In addition, pursuant to 18 U.S.C. § 2705(b), I would request the Court order the Target Providers described in Attachment A not to notify any other person, including the subscribers or customers of the account(s) listed in Attachment A, of the existence of this warrant, its contents, and any information provided in response thereto, until one year from the date of this warrant, and to continue to maintain the accounts in an open and active status so as not to disrupt this ongoing investigation.

54. As described above, this warrant relates to an ongoing investigation of violations of 18 U.S.C. § 875(c) [Interstate Communications] and 18 U.S.C. § 2261A(2) [Cyberstalking]. Targets of such investigations frequently engage in extensive online social networking, including efforts to discover any potential ongoing investigations relating to them. This investigation is neither public nor known to all of the targets of the investigation, and its disclosure may alert the targets to the ongoing investigation. Indeed, at this time the targets of the investigation believe that their true identities are unknown, due to registering the Target Accounts under false names, and notification would alert the targets of the investigation that the United States has obtained information that may result in their identification. Additionally, the United States is investigating threats of violence, including threats to rape adult female victims and unborn children, and the targets have expressed ideations of committing similar future acts of violence. Notification of this investigation provides an opportunity for the targets to flee prosecution. Additionally, the majority of the evidence in this investigation is stored electronically. If alerted to the investigation, the targets under investigation could destroy any evidence saved on their electronic devices, including information saved to their personal computers, as targets have done in similar types of investigations when alerted to the investigation. Moreover, notification of the subscriber or customer will likely result in the targets changing patterns of behavior and/or discontinuing use of a particular means for committing the crime, therefore seriously jeopardizing the investigation.

55. Accordingly, there is reason to believe that notification of the existence of the warrant, its contents, and the information requested therein, will seriously jeopardize the investigation, including by giving targets an opportunity to flee or continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, or notify confederates. *See* 18 U.S.C. §§ 2705(b)(2), (3), and (5).

REQUEST TO MAINTAIN ACCOUNTS

56. Request to Maintain Account: I would further request the Court to order the Target Providers to continue to maintain the Target Accounts listed in Attachment A in an open and active status for one year from the date of this warrant so as not to disrupt this ongoing investigation.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

57. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Meta to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

58. Based on the foregoing, I request that the Court issue the proposed search warrant.

59. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving it on Meta Platforms, Inc. Because the warrant will be served on Meta Platforms, Inc., who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

Casey S. Cox
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to ~~before me~~ by telephone on the 25th day of October, 2024

SUSAN E. HUNTSMAN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with Facebook accounts 61550038546748, 100027927924028, and 1843835659471281 that are stored at premises owned, maintained, controlled, or operated by Meta Platforms, Inc., a company headquartered in Menlo Park, CA.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Meta Platforms, Inc. ("Meta")

To the extent that the information described in Attachment A is within the possession, custody, or control of Meta, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Meta, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Meta is required to disclose the following information to the government for each user ID listed in Attachment A:

(a) All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.

(b) All activity logs for the account and all other documents showing the user's posts and other Facebook activities from 1/1/2024 to current date.

(c) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them from 1/1/2024 to current date, including Exchangeable Image File ("EXIF") data and any other metadata associated with those photos and videos;

(d) All profile information; News Feed information; status updates; videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;

(e) All records or other information regarding the devices and internet browsers associated with, or used in connection with, that user ID, including the hardware model, operating system version, unique device identifiers, mobile network information, and user agent string;

(f) All other records and **contents of communications and messages** made or received by the user from 1/1/2024 to current date, including all Messenger activity, private messages, chat history, video and voice calling history, and pending "Friend" requests;

(g) All "check ins" and other location information;

(h) All IP logs, including all records of the IP addresses that logged into the account;

(i) All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked";

(j) All information about the Facebook pages that the account is or was a "fan" of;

(k) All past and present lists of friends created by the account;

(l) All records of Facebook searches performed by the account from 1/1/2024 to current date.

(m) All information about the user's access and use of Facebook Marketplace;

(n) The types of service utilized by the user;

(o) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);

(p) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;

(q) All records pertaining to communications between Meta and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken.

Meta is hereby ordered to disclose the above information to the government within **14** days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and/or instrumentalities of violations of 18 U.S.C. § 875(c) [Interstate Communications] and 18 U.S.C. § 2261A(2) [Cyberstalking], those

violations involving John Gregory Garza [the Target], aka "Mikey Chuddington", aka "Mike Chuddington", aka "Mike Chudington", aka "Chud Rosenberg", and aka "Cole McHale" and occurring after 1/1/2024, including, for each Account or identifier listed on Attachment A, information pertaining to the following matters:

(a) All records, images, communications, or information, however maintained, reflecting interstate communications containing any threat to injure or intimidate or interest in intimidating or injuring any victim, identified or not yet identified;

(b) All records, images, communications, or information, however maintained, reflecting threats or sexual violence against women or children, threats or violence against minority members or other non-white persons, murders and mass shootings.

(c) All evidence indicating any plans or intentions of carrying out any violent threat, such as text, photographs, or video.

(d) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the Target Offenses and to the Facebook account owner;

(e) Evidence in the form of communications that contain "true threats" including threats to injure [true threats] based on a bias of a protected group;

(f) Evidence indicating how and when the Accounts were accessed or used, to determine the geographic and chronological context of account access, use,

and events relating to the crime under investigation and to the email account owner;

(g) Evidence indicating the Accounts owner's state of mind as it relates to the crime under investigation;

(h) The identity of the person(s) who created or used the Accounts including records that help reveal the whereabouts of such person(s).

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Meta Platforms, Inc. ("Meta"), and my title is _____.

I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Meta. The attached records consist of

_____

_____

_____

_____

[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Meta, and they were made by Meta as a regular practice; and

b. such records were generated by Meta's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Meta in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Meta, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature